RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: STR-W02

IMPLEMENTING A QUANTITATIVE CYBER RISK FRAMEWORK: A FINSRV CASE STUDY

Jack Freund, Ph.D.

Director, Cyber Risk
TIAA
@jackfreund3

Impetus for Cyber Risk Framework

3 OpRisk Integration
- OpRisk Framework under development
- Focus on high-level, business risk
- Political pressure to adopt

1 Staffing Levels
- Small staff
- Opportunity for one-time uplift
- Level staffing afterwards

Cyber Risk Framework

5 Solution requirements
- Which risks and regulations apply?
- What control requirements apply?
- Need control governance that scales from Board level to technician level
- Rigor and justification for risk ratings
- Integration with OpRisk → ability to scale from small to large problems

2 Acquisitions Strategy
- Several large and small acquisitions on the horizon
- No additional staffing as a result

4 Other Pressures
- Regulatory expectation for granular view of risk
- Capital Reserve Allocations
- Cyber insurance

Overview of Cyber Risk Framework

	1	2	3	4
Framework	Identification	Controls	Assess	Treat
Process	**Risk Classification**	**Policy Standards Procedures**	**Control Assessment**	**Break Management**
	• Used to determine the inherent risk • Drives the level of controls needed • Maps risks to resources • Maps regulations to resources • Each resource needs a current risk classification	• Prescribes only the controls needed to manage the resource's inherent risk or regulations • Avoids over-controlling the environment • Clear guidance on what control is needed for the resource	• Assess if a control is in place per the prescribed procedure • Leverage automation where possible to reduce assessment fatigue • Provide workflow to collect evidence and automate	• Prioritize the remedy of breaks based on the risk to the resource • Allows analysis of breaks • Simplified workflow to action a break

Control Framework Overview

The Information Technology Policy and Control Framework allows articulation of requirements for technical configurations, processes, and behaviors throughout the IT organization.

	Definition	Example
1 Policy	• A collection of standard statements indicating Purpose, Scope, Objectives and Control (or Compliance) requirements that is not relative to a specific technology but is ubiquitous throughout all of IT and organized by high level directives.	• IT Policy
2 Standard	• A standard is a statement designed to meet the security expectations and requirements of our regulators, auditors, and institutions. They are not statements of capability but expectations on our organization to which we must adhere.	• Users must not be able to construct passwords that are identical to those used the last twelve (12) times they have changed their password.
3 Procedure	• An instruction or set of instructions which inform staff of how IT standards are to be implemented. Procedures also detail the testing criteria used to measure a passing outcome or a break during an assessment. A procedure can define a technical configuration setting or define requirements for a process.	• Windows 2008 R2 and 2012 R2 Member Servers will be set to record the previous 12 passwords.

What — General/ Descriptive

How — Specific/ Prescriptive

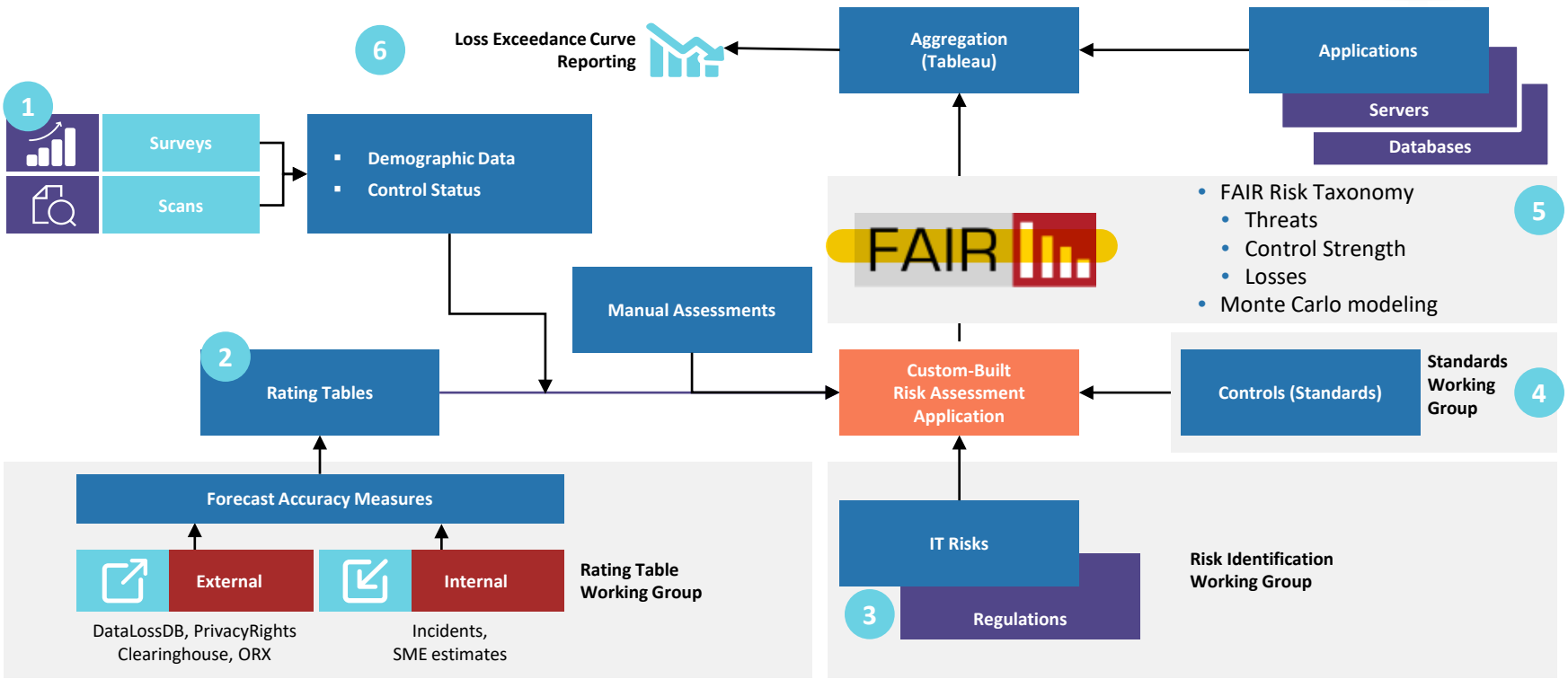
Authoritative Sources

Authoritative Sources map regulatory guidance to IT standards, which aids in the identification of gaps. Authoritative Sources should be regularly reviewed for completeness and appropriateness.

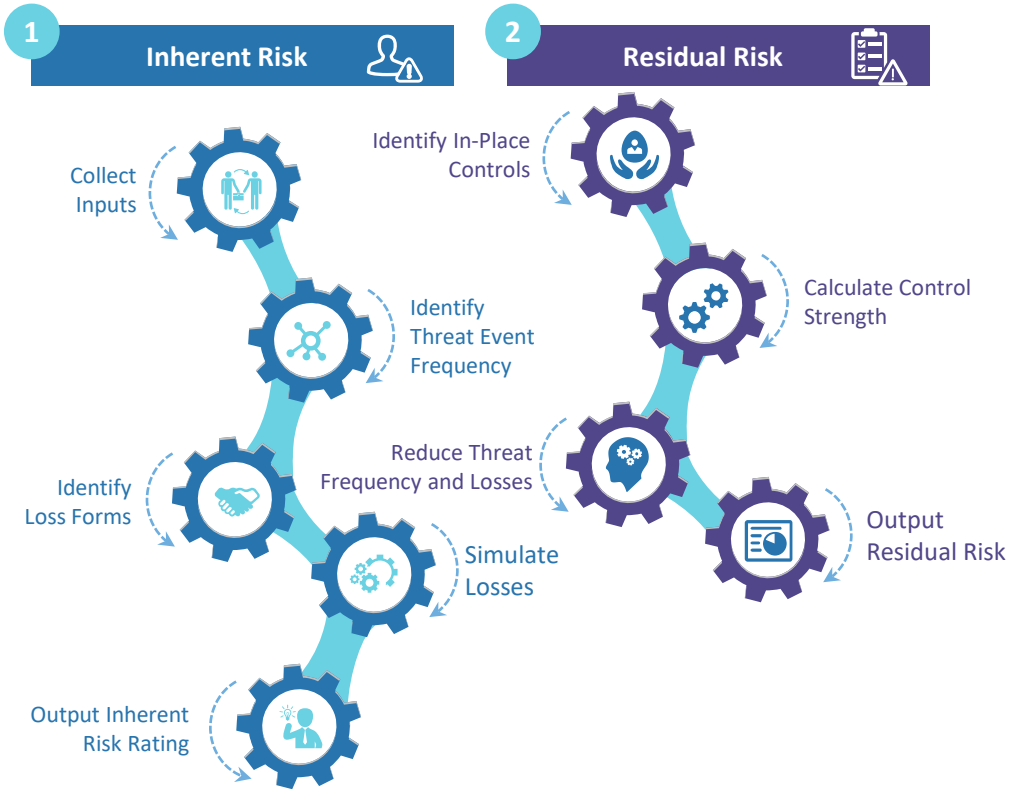
1	Regulators	Auditors	Customers
	Federal Reserve Bank of Boston, FINRA, Office of the Comptroller of the Currency, U.S. Department of the Treasury	PwC, KPMG	Institutions, Individuals
2 Authoritative Sources	• FFIEC • Sarbanes-Oxley • NIST Cyber Security • State Privacy Laws	• SSAE16 Type 2 • COBIT • NIST • ISO	• 23 NYDFS 500 • FACT ACT – Red Flag • SEC OCIE • National Futures Association
3 Standards Groupings/Control Programs	• Cybersecurity Management • Cyber Risk Management • IT Personnel Security • IT Physical Security • IT Operations Management	• IT Security Monitoring & Response • IT Communications Management • Workforce Access Control • IT Network Security • Supplier Management	• IT Application Mgmt. • IT Business Continuity • IT Compliance and Privacy • IT Event and Incident Management • Customer Authentication

Authoritative Sources are mapped to IT standards to ensure they meet the expectations of regulators, auditors, and customers.

IT Risk Central Overview

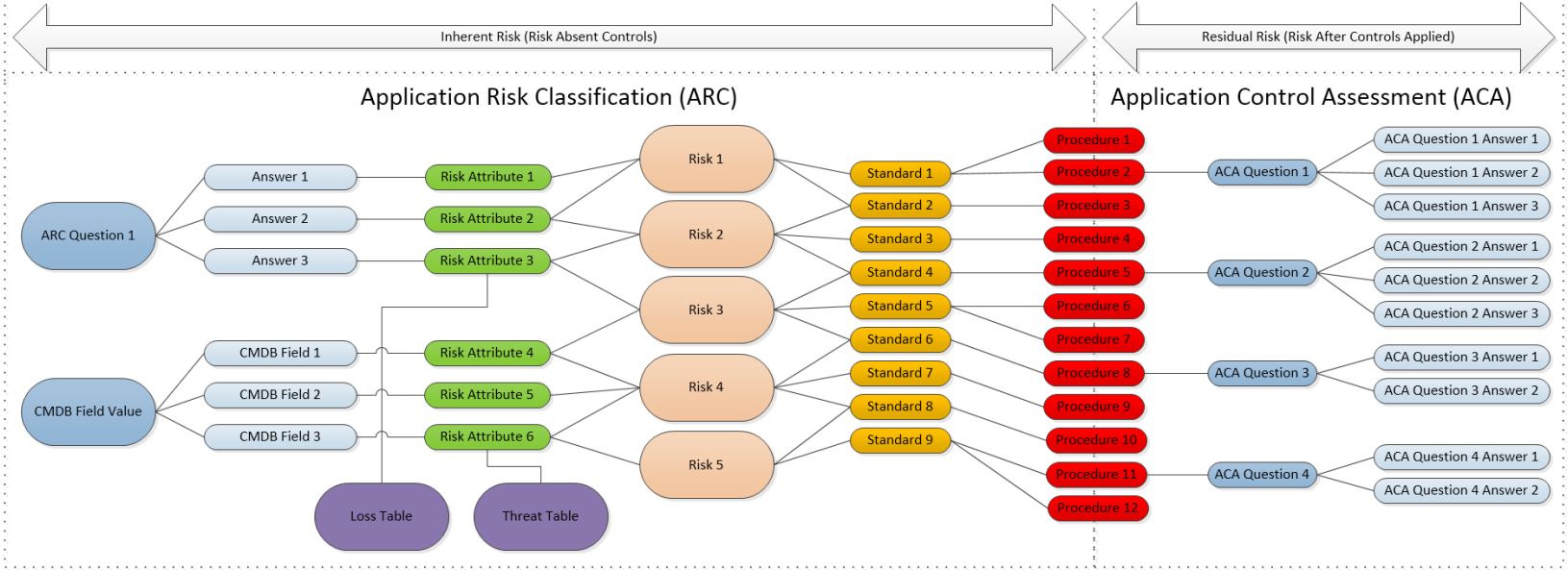


Risk Assessment Process, Scope, & Metrics



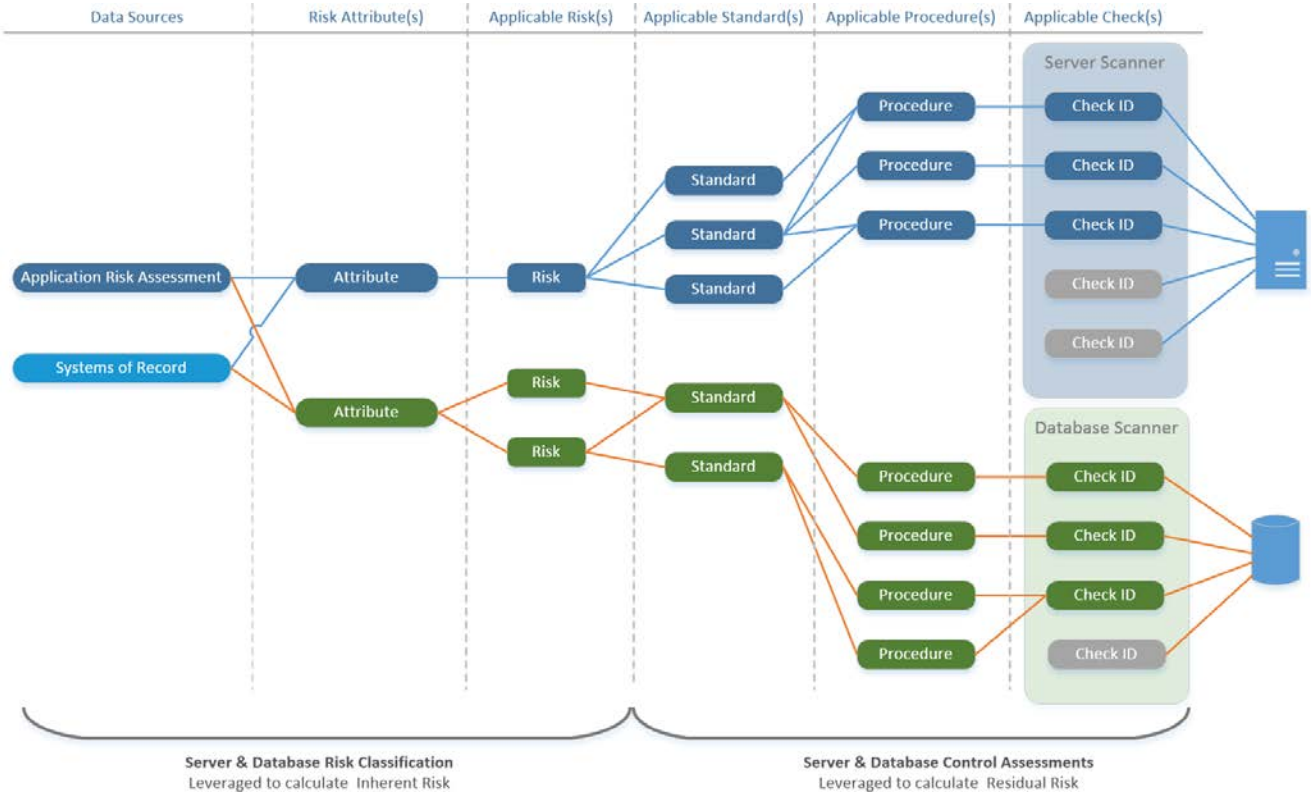
			3 Ex. Scope		4 Risk Visibility Metrics (KRIs)			Risk Operation Metrics (KPIs)	5
	Assessment	Type	% Resources	% Controls	% in Appetite	% Completed Within SLA	Completed YTD		
Business	Applications	I							
		R							
	IT Services	I/R							
	Projects	I/R							
Infrastructure	Servers	I							
		R							
	Databases	I							
		R							
	Network	I							
		R							
	Workstations	I							
		R							
	IOT	I/R							
	Container	I/R							
	Cloud	I/R							
Third Party/ Data Centers	Facilities	I/R							
	Suppliers	I/R							
	Subsidiaries	I/R							
	Data Transfers	I/R							

Application Risk Assessment Details



ARC Question	ARC Answers	Risk Attribute	Risk	Standard	Procedure	ACA Question	ACA Answers
How often in the course of a year is the application modified or changed?	• Once a year or less • Once a quarter • Every other month • Once a month • More than once a month	• Resource Change Frequency : 1 or Less • Resource Change Frequency : 4 • Resource Change Frequency : 6 • Resource Change Frequency : 12 • Resource Change Frequency : > 12	Erroneous change in an application or system by an authorized user	All internal development efforts must follow the Systems Development Life Cycle methodology and Change Management Processes.	All internal development efforts must follow the Systems Development Life Cycle methodology and Change Management Processes.	Is the Change Management process followed when changes are made to the application or other dependent components?	• Yes • No

Infrastructure Risk Assessment Details



Server & Database Risk Classification (SRC/DRC):

- Determine the applicability of IT Standards & Technical Procedures relevant to each server and database
- Informs inherent risk calculations

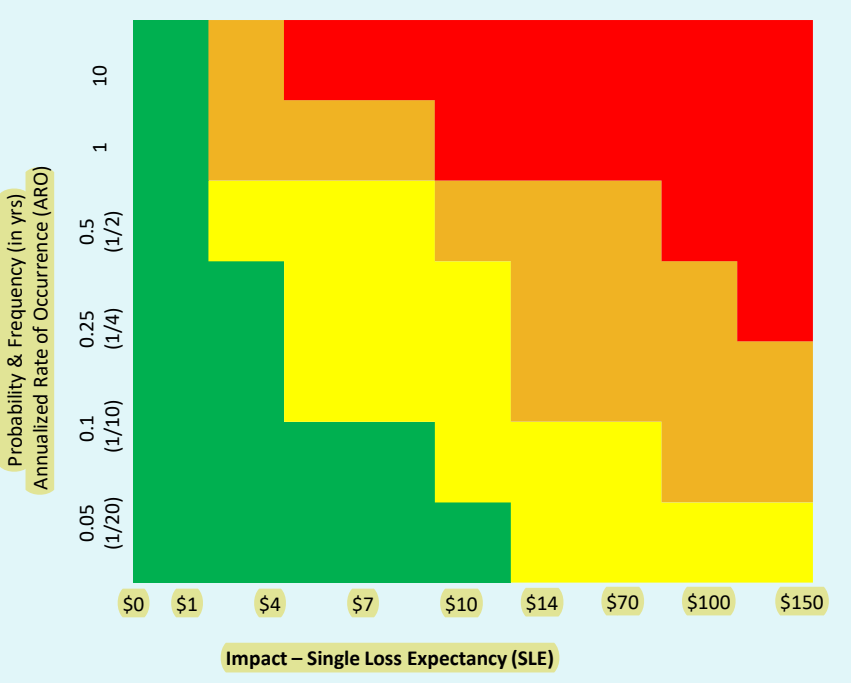
Server & Database Control Assessment (SCA/DCA):

- Evaluate servers and databases against the relevant Technical Procedures
- Create breaks for deviations
- Informs residual risk calculations

Risk Ratings – Translating Quant to Action

1

Example Cyber Risk Heatmap



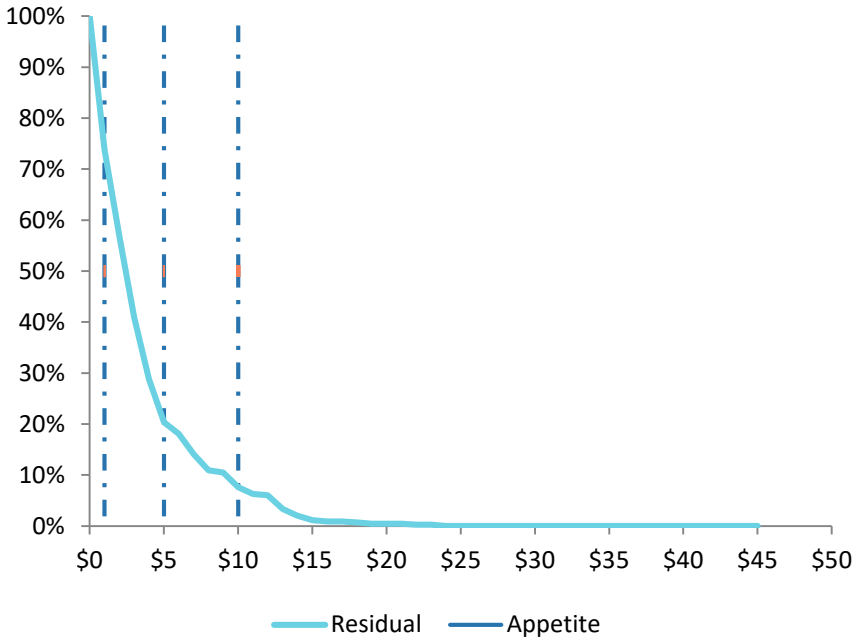
2

Ranking	ALE	Behavior
Critical	> $14	All hands on deck, cost of resolution is a nonfactor, daily meetings (or more frequent) tracking to resolution
High	> $8	Gains attention of upper management; plans are made to track concern to resolution in current or next period
Moderate	> $1	Willingness of management to adjust plans and reallocate resources in the current or next few planning periods to remediate
Low	< $1	Infrequent monitoring/review to ensure risk does not escalate

Aggregate Risk Appetite Reporting using LECs

1

<Quarter> <LOB> LEC – Per Incident Loss Projections



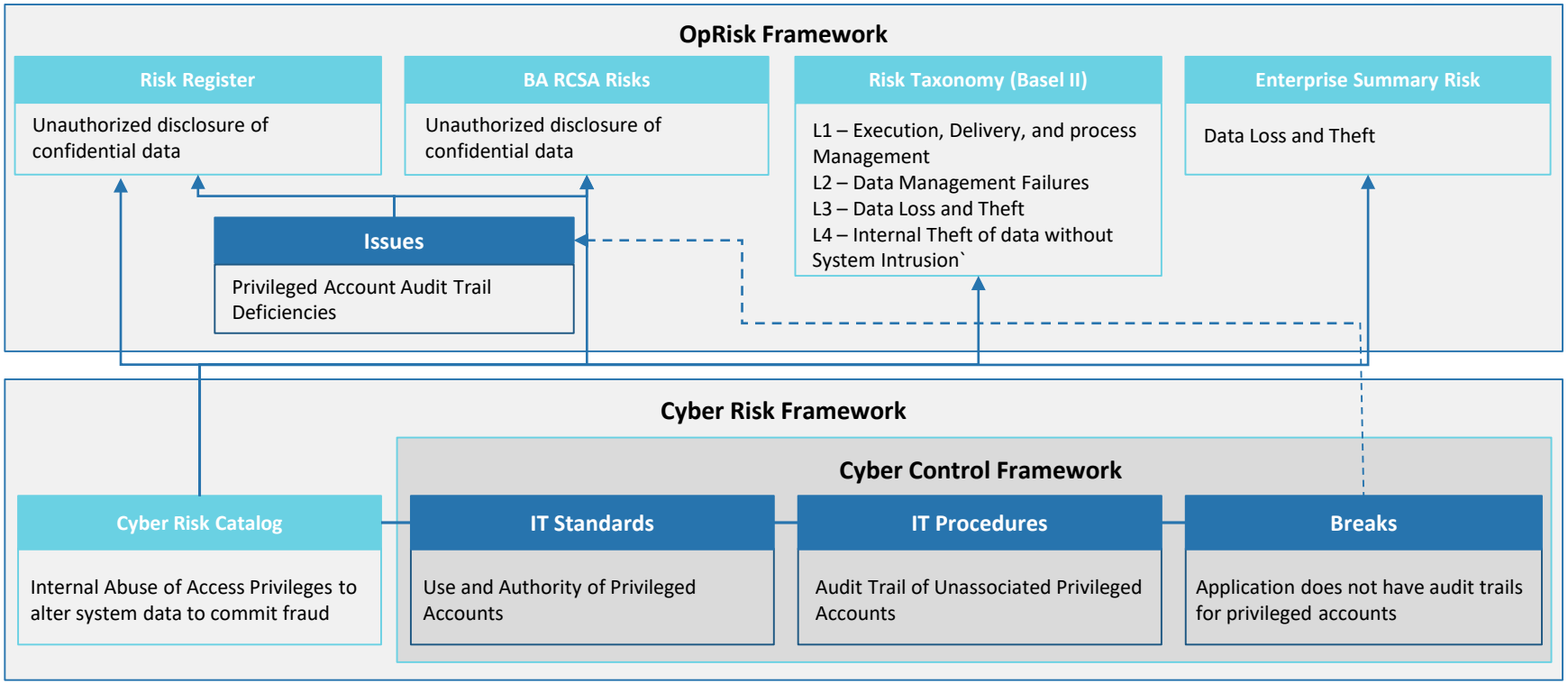
2

Appetite	Probability of Exceeding Appetite	# of Apps that Exceed Appetite
$1	75%	25
$5	18%	15
$14	3%	8

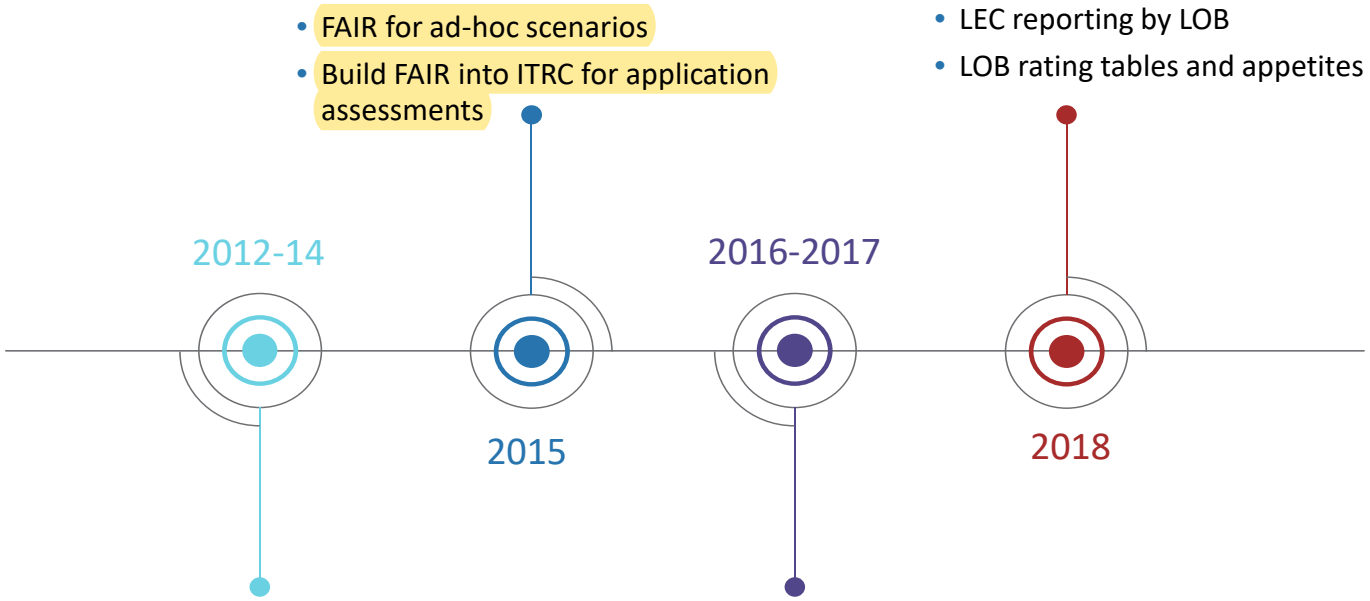
You can use multiple appetite thresholds to begin socializing risk appetite

- 75% of <LOB> applications could contribute to a technology risk incident that exceeds the appetite due to having a residual risk (after considering in-place controls) higher than $1
- Residual risk graph represents 500 critical/high inherent risk applications that completed the control assessment
- Reduction of residual risk can be accomplished through remediation of control gaps

OpRisk Integration



History of Cyber Risk Quant



- FAIR for ad-hoc scenarios
- Build FAIR into ITRC for application assessments

- LEC reporting by LOB
- LOB rating tables and appetites

- FAIR for “security exceptions” and Issue Management

- FAIR in ITRC assesses more IT Resources
- Aggregate reporting using risk appetite and Loss Exceedance Curves
- FAIR assessed by the Model Risk Management program

Quant Cyber Risk Justification

OpenGroup

- Independent IT Standards organization
- OpenFAIR Body of Knowledge (Since 2009)
  - Risk Ontology
  - Risk Analysis Process
- Individual Analyst Certification (Since 2013)
- FAIR/ISO Cookbook standard that outlines the process to integrate FAIR into any other security standard

NIST Cybersecurity Framework (CSF)

- NIST recognized FAIR as a complementary standard to add economic dimensions to impact assessments (under industry resources)

Federal Reserve, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC)

- In the ANPR sent jointly by these three agencies, they are looking to for a consistent, repeatable, methodology to support measurement of cyber risk. FAIR was one of two methods identified
- Jay Restel from the Federal Reserve Bank of Cleveland identified publically that FAIR will be an important component of cyber risk measurement for large banks

Payment Cards Industry Data Security Standard (PCI-DSS)

- PCI's Risk Assessment Guideline in section 3 recommends compliance with NIST, ISO, and recommends FAIR as a risk framework to complement these two standards

FAIR Book (2014)

- Published by TIAA employee and creator of FAIR
- Book was inducted into the Cyber Security Cannon in 2016 (Books all cyber security professionals should read)
- Referenced in 2016 book How to Measure Anything in Cybersecurity Risk (Douglas Hubbard) as a model that can be used to measure cyber risk. Douglas's books on risk measurement are required reading for the Society of Actuaries Enterprise Risk Management exams

FAIR Institute (2013)

- Non-profit organization established in 2013 to promote the practice of cyber risk measurement and quantification
- FAIR is the primary methodology supported by the Institute

Key Takeaways and Application